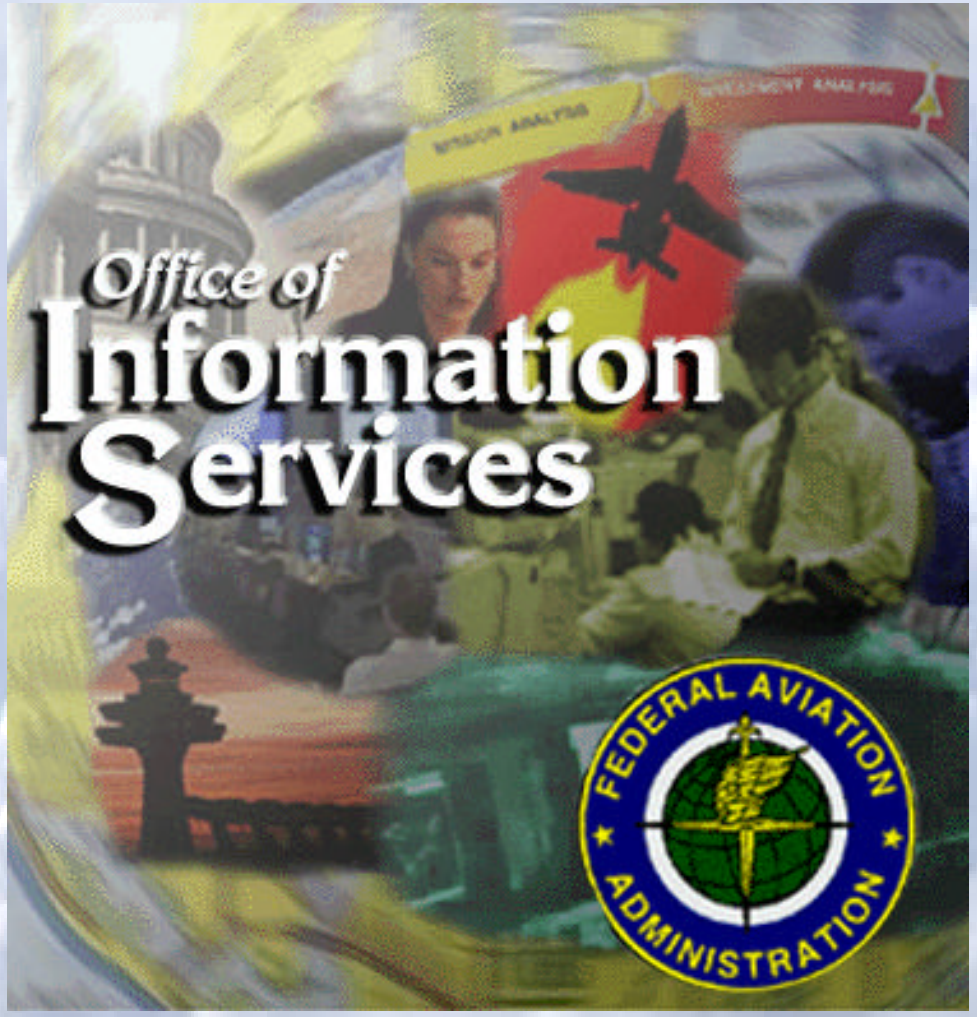


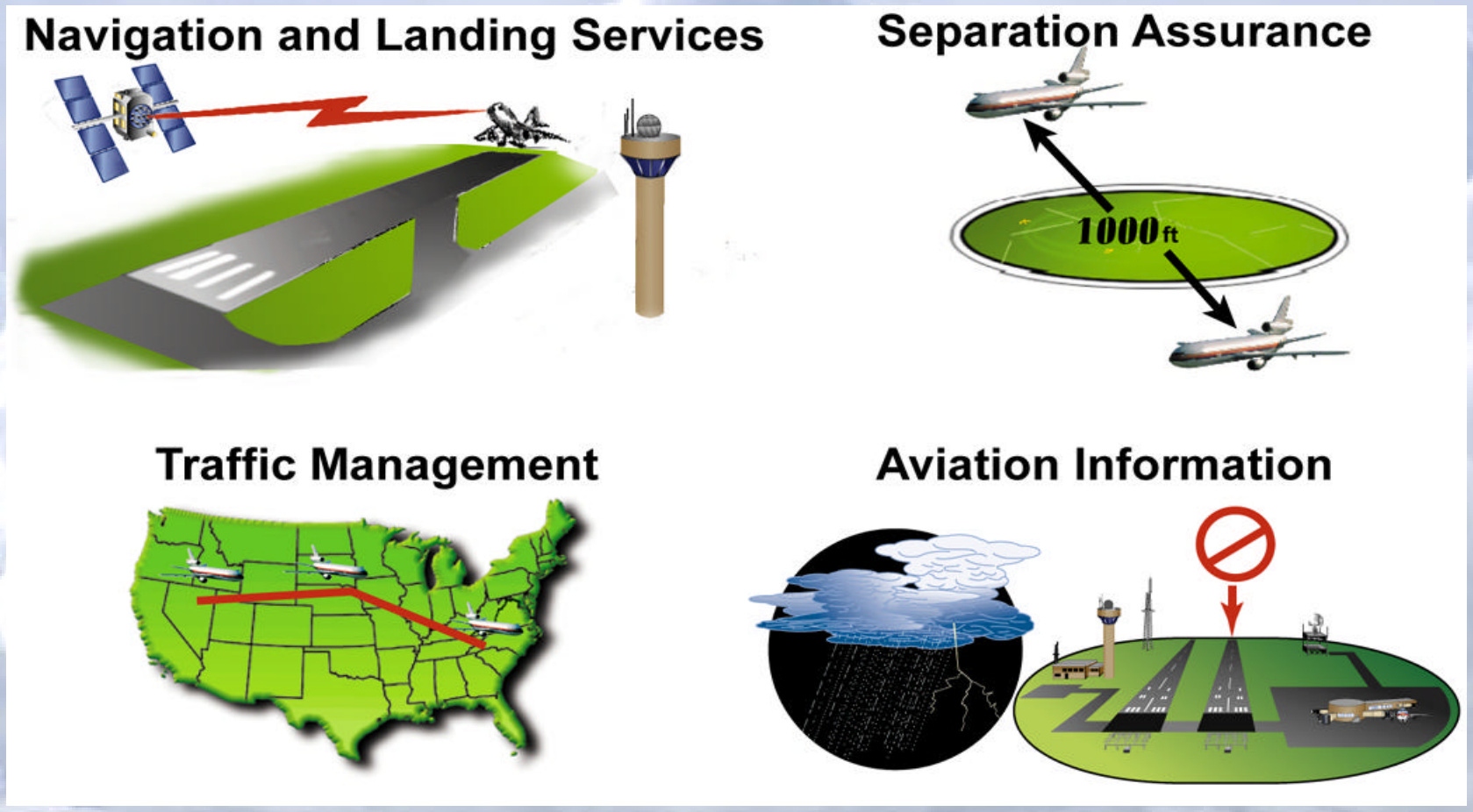
System Level Protection Profiles: A Mechanism for Defining ISS Requirements for the National Airspace System (NAS)

Marshall Potter
Chief Scientist for
Information Technology (AIO-4)
Federal Aviation Administration
800 Independence Ave, SW
Washington, DC 20591
(202) 267-9878

Version 3 2/28/01

March 7, 2001

National Airspace (NAS) System Services



Future Environment

- **Increasing cyber terrorist threat and hostile hacker attacks on information networks**
  - **Some new/recent attacks/vulnerabilities were not even considered as weaknesses before they were recently found:**
    - **Distributed Denial of Services (DDoS)**
    - **Foreign Air Traffic Systems have suffered major outages**
    - **Phantom Controllers**
  - **FAA specific systems will continually need to be modified to be kept "secure" in this changing environment. (e.g.)**
    - **Controller Pilot Data link Communications (CPDLC)**
    - **NAS Infrastructure Management System (NIMS)**
    - **FAA Telecommunications Infrastructure (FTI)**
  - **Move from Proprietary, Legacy Systems to Open, Interconnected, COTS based Systems of Systems**

Impacts of ISS Mechanisms

- **Increased latency**
- **New costs**
  - **Both Implementation and O&M**
- **Impeded access**
  - **Security can lock out proper users**
- **Increased system complexity**
  - **Impacts on acquisition costs and acceptance testing**
- **Union issues**

Multiple Views and Models

Process Model
(how to)

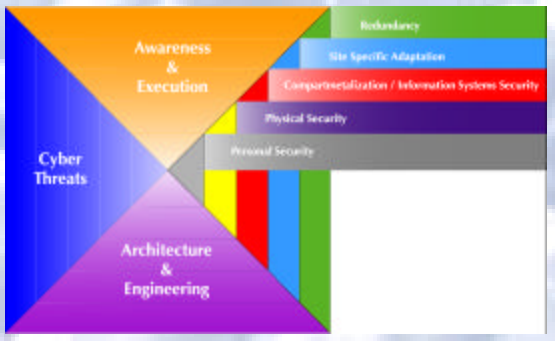
SYSTEM PROTECTION THREAD

PHYSICAL SECURITY THREAD

PERSONNEL SECURITY THREAD

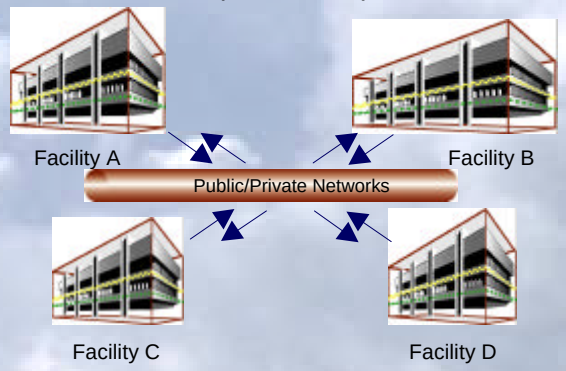
Integrated Facility Certification
(IFC)

Structural Model
(strategy)



Information Systems Security Goals

Operational Model
(to be state)

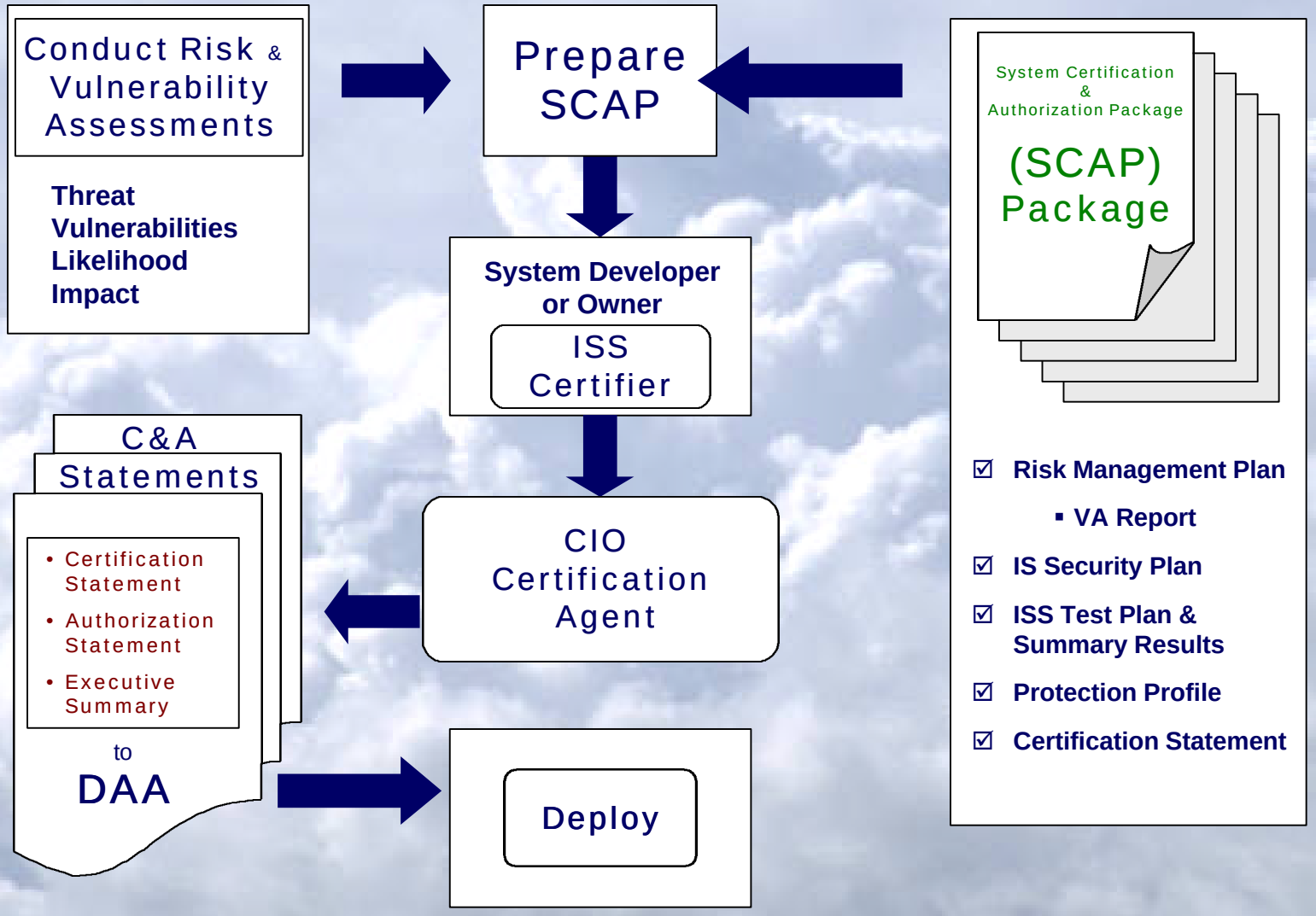


D.J. Mehan, "Information Systems Security: The Federal Aviation Administration's Layered Approach, TR News, Nov-Dec 2000, No. 211

Previous FAA Protection Profile Efforts

- Two PPs written by CAASD for FAA (FTI and NIMS)
- User Request Evaluation Tool (URET) PP in development
- Information Systems Security Architecture (version 1.1 was issued in September 2000, version 1.2 will be issued in April/May 2001 and Version 2.0 in September 2001)
- FAA Order 1370.82 ISS Program defines Security Certification and Authorization Package (SCAP) as the package that is presented to the DAA for final authorization of the system. The SCAP includes the ISS Plan, vulnerability assessment report, risk assessment, security test plan, security test results, disaster recovery and contingency measures and ISS certification and authorization statements and protection profiles.

System Protection Thread



SCAP RELATIONSHIP TO PP

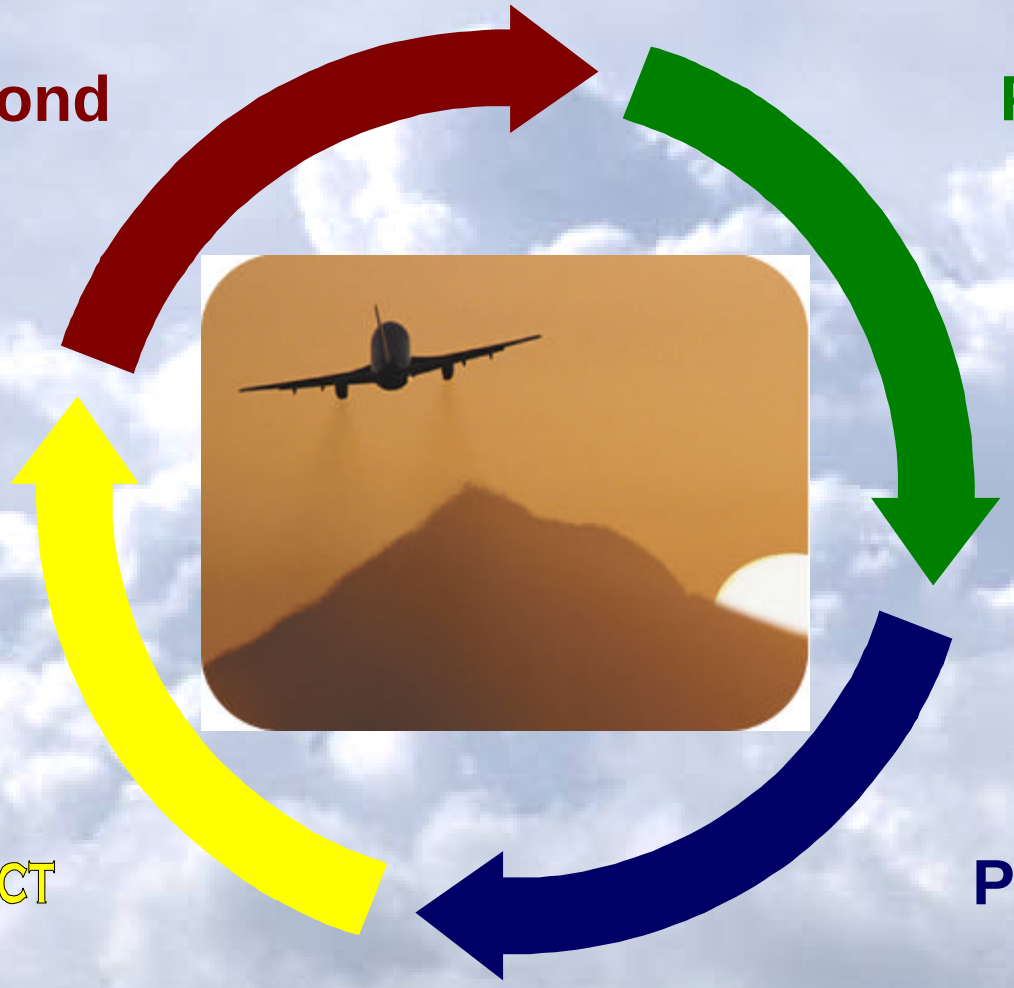
- **Protection Profiles are a combination of security requirements, including assurance and functional requirements, with the associated rationale and target environment to meet identified security needs.**

- (FAA Order 1370.82 Appendix 1, p.4)

FAA Findings

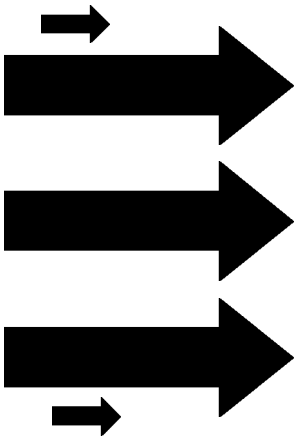
- NIST guidance is to use Protection Profiles as a means of developing security requirements
- The Common Criteria (ISO Standard 15408 June 99) needs adaptation, interpretation and extension if we are going to use it on a “system of systems”
- National Information Assurance Partnership (NIAP) CC ToolBox may help automate the writing of PPs

FAA's Information Systems Security Approach



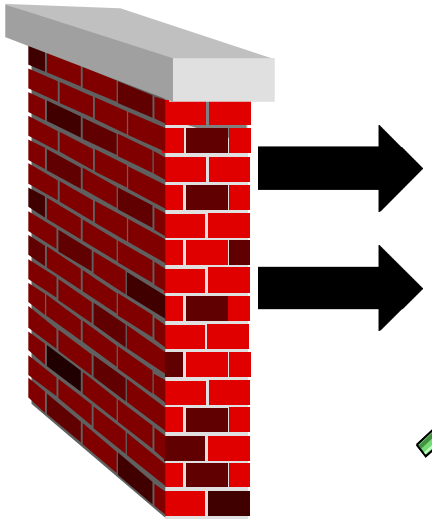
Current & Future Architecture & Engineering Efforts

Attack



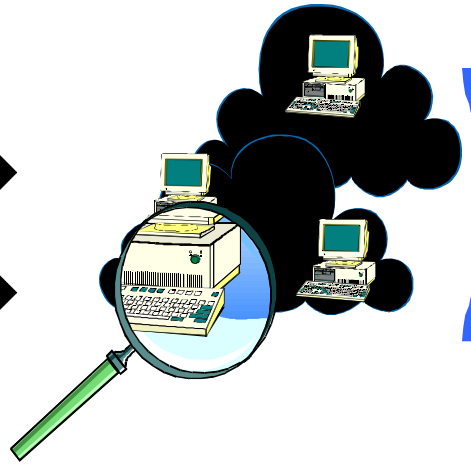
- Malicious Software
  - Viruses
  - Trojan Horses
- Data Insertion / Modification / Deletion
- Illegally Advance Privileges
- Denial of Service
  - Flooding

Protect



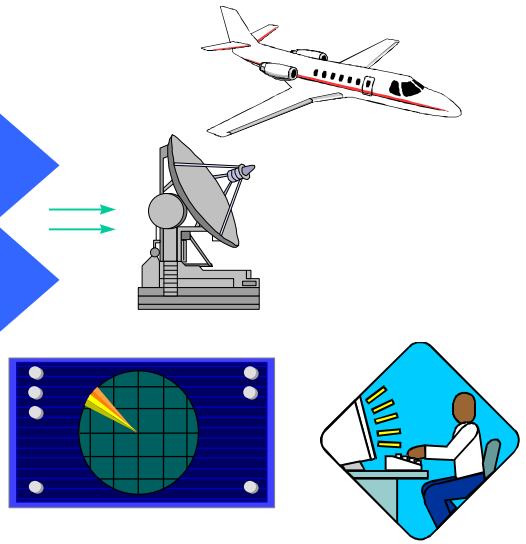
- Secure Configuration
  - Shut off unnecessary services (email/web)
  - Issue file privileges
- User Identification & Authentication
  - Passwords/Biometrics
- Message Authentication
- Private Key Infrastructure
- Virtual Private Networks (VPN)

Detect



- Host & Network Intrusion Detection
- Malicious Code Detection
- Intelligent Agent Distributed Response Units
- Computer Security Incident Response Capability (CSIRC)

Respond



- Tighten Access Control
- Identify Attack Source & Skill Level
- Re-route Traffic
- Eliminate Attack Process
- Damage Assessment / Recovery
- Malicious Code Eradication

Protect, Detect, and Respond components will be integrated and managed by a Information System Security Architecture (ISSA)

How does the CC contribute to our needs

- **Provides a general model for us to use and provides a degree of commonality in defining requirements**
- **Helps define desired security behavior and requirements**
  - Functionality is effectively and correctly implemented
- **Addresses products & small systems (system components)**
  - However needs to be expanded for large systems or for systems of systems

Protection Profiles
A Means to Developing Requirements

- **Use PPs to help define NAS ISS requirements**
- **Use PP framework to ensure uniform security engineering among NAS programs**
- **Make it easier for NAS programs to be secure**
  - Helps write better requirements
  - Provides guidance and tools for NAS programs to write "derivative" and "subordinate" PPs
- **Provides mechanisms for Stakeholder communication**

Can We Use the CC Toolbox?

- **Increase usefulness of produced products**
  - We hope to use it in acquisitions
  - We however need to determine a useful format
  - Who will be expected to read and use the PP?
- **Enhance uniform security engineering among NAS Products**
  - Build common elements into the tool
  - Force common analysis through the tool's questions
  - Encourage thinking of mutual protection

Project Deliverables for FY 01

- Create a top-level or “master” PP for the NAS
- Produce instructions for NAS systems to write “derivative” or “subordinate” PPs
- Create worked examples

Project Structure

- **Writing Group**
  - 1.5 FTE @ MITRE (Marshall Abrams & Joe Veoni)
  - NIAP (Kris Britton)
  - Selected FAA participants
- **Reviewers**
  - PP Steering Group and major stakeholder representatives
- **Steering Group**
  - Oversight of Writing Group